REMARKS

Claims 1-20 are pending in the application. Reconsideration of the rejected claims in view of the above amendments and the following remarks is respectfully requested.

35 U.S.C. § 112, 2nd paragraph, Rejection

Claims 9, 11, 13 and 17-20 were rejected under 35 U.S.C. § 112, 2nd paragraph, for allegedly being indefinite. This rejection is respectfully traversed.

The Examiner asserts that claims 9, 11 and 17-20 are rendered indefinite because they recite "clock cycle" and because "the amount of time is not constant". Applicant respectfully disagrees that these claims are indefinite. Paragraphs [0007] and [0009] of the instant published application No. 2002/0101985 explains that the single hardware cycle may take several clock cycles or just one clock cycle. The noted claims merely recite which is disclosed in the specification. Furthermore, the Examiner has not explained how the use of the term "clock cycle" would render the claims unclear to one having ordinary skill in the art having read the specification.

The Examiner asserts that claim 13 is indefinite and does not further limit the invention. Applicant respectfully disagrees that this claim is indefinite. Paragraph [0007] of the instant published application No. 2002/0101985 defines combinational logic as logic functions whose outputs depend solely on their inputs. The noted claims merely recite which is disclosed in the specification. Furthermore, the Examiner has not explained how the use of the noted language would render the claims unclear to one having ordinary skill in the art having read the specification.

In view of the above, Applicants respectfully request withdrawal of the above-noted rejection under 35 U.S.C. § 112, 2nd paragraph.

35 U.S.C. § 102 Rejection

Claims 1-20 were rejected under 35 U.S.C. § 102(e) for being allegedly anticipated by U.S. Patent No. 6,870,929 to GREENE. This rejection is respectfully traversed.

In order to establish a *prima facie* case of anticipation under 35 U.S.C. § 102, a single prior art reference must disclose each and every element as set forth in the subject claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). Applicants respectfully submit that a *prima facie* case of anticipation cannot be established because GREENE fails to teach each and every element of the claims.

More particularly, independent claim 1 recites, *inter alia,*

> a first register storing data to be encrypted or decrypted;
> a second register for receiving data which has been encrypted or decrypted; and
> combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

Additionally, independent claim 16 recites, *inter alia,*

> a first register that stores data to be encrypted or decrypted;
> a second register that receives data which has been encrypted or decrypted; and

> combinational logic that performs computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle,
> wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read.

Finally, independent claim 19 recites, *inter alia,*

> a first register that stores data to be encrypted or decrypted;
> a second register that receives data which has been encrypted or decrypted; and combinational logic that performs computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle,
> wherein the single hardware cycle comprises several clock cycles.

Applicants submit that GREENE does not disclose or even suggest at least these features. Applicants acknowledge that GREENE discloses an arrangement which utilizes an encryption circuit 102, an input buffer 104 and an output buffer 108 (see col. 5, lines 4-12). Applicants also acknowledge that GREENE discloses that the encryption circuit 102 utilizes "data encryption algorithms such as DES and Triple DES, or any of various secure hash algorithms" (see col. 6, lines 58-62). However, Applicants submit that GREENE does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

The Examiner explains that the disclosed encryption circuit 102 of GREENE is same as the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register <u>in a single hardware cycle</u>. Applicants respectfully disagree. An encryption circuit is not the *per se* same as combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle. As explained on paragraph [0005] of the instant published application No. 2002/0101985, conventional processing of crypto-functions require many clock and hardware cycles. As such processing typically occurs in an encryption circuit, the Examiner's apparent or implicit belief that all encryption circuits perform computation iterations of the crypto-function in a single hardware cycle lacks any support in the prior art.

Furthermore, while the Examiner has specifically pointed to col. 4, line 58 to col. 5, line 13 as disclosing the recited computation, the Examiner has failed to fully appreciate the fact that the noted language is entirely silent with regard to the terms "computational logic" and "crypto-function" and merely states the following:

> Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.
>
> Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

There is simply no such disclosure in the above-noted language of GREENE and the Examiner has not demonstrated otherwise.

Thus, Applicants respectfully submit that independent claims 1, 16 and 19, and claims 2-15, 17, 18 and 20, which depend from claims 1, 16 and 19 are allowable.

For example, the Examiner is not correct that col. 7, lines 7-21 and col. 7, line 62 to col. 8, line 4 discloses that the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times (claim 5). The noted language merely discloses the following:

> In FIG. 4A, data blocks from different contexts are given a particular letter designation and number designation. The letter designation indicates a context of origin, the number designation indicates how many blocks have previously been processed for the context in question. Thus, a first context can provide data block A1, followed by data block A2, followed by data block A3, etc. Further, if it is assumed that CBC is employed, the encrypted form of data block A1 (designated as E[A1]) is an input that is used together with data block A2 to encrypt data block A2.
>
> In general, each context will have its own encryption/decryption key (or, in the case of Triple-DES and similar algorithms, set of encryption/decryption keys). The keys for all active contexts are stored and retrieved at appropriate times as seen below.
>
> A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority. Further, one skilled in the art would recognize that the feedback loop in an encryption circuit would be disabled on this cycle to prevent the E_{KB} [B3] value from being combined with the E1 value.

The Examiner is also not correct that col. 7, lines 7-21 and col. 8, lines 6-32 discloses that the combinational logic performs mixing, permutation and key-dependent substitution in each round (claim 6). The noted language merely discloses the following:

In FIG. 4A, data blocks from different contexts are given a particular letter designation and number designation. The letter designation indicates a context of origin, the number designation indicates how many blocks have previously been processed for the context in question. Thus, a first context can provide data block A1, followed by data block A2, followed by data block A3, etc. Further, if it is assumed that CBC is employed, the encrypted form of data block A1 (designated as E[A1]) is an input that is used together with data block A2 to encrypt data block A2.

In general, each context will have its own encryption/decryption key (or, in the case of Triple-DES and similar algorithms, set of encryption/decryption keys). The keys for all active contexts are stored and retrieved at appropriate times as seen below.

In an alternate embodiment, a system may include as many contexts as there are pipeline stages. Each context can be accessed sequentially. In the event a context does not include a data block, a read from the input buffer and write to the output buffer can be suppressed.

In this way, an encryption system can provide an encrypted data block in each system cycle for feedback-type encryption. This is in contrast to a conventional approach that may supply a first data block of a sequence to an encryption circuit and then supply the second block a predetermined time later, limited by the latency of the encryption process on the first data block. Thus, the present invention can process a data block on each system cycle (provided sufficient contexts are active) even when the encryption function includes a feedback loop.

While the above description has described the particularly useful application of the invention to encryption, the described embodiments could also be utilized in other computations, such as modular exponentiation, as but one example. As one very particular example, if the method described in the background above is employed to compute y=(A^e)mod n, a modular multiply computation circuit (in place of the encryption circuit 102) could provide the yy=(yy*aa) mod n operation and/or the aa=(aa*aa) mod n operation. Of course, the scheduler operation could be adjusted to ensure that the yy=(yy*aa) mod n operation is performed only for iterations corresponding to an "e" bit value equal to one.

The Examiner is also not correct that col. 7, lines 51-67 discloses that the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation (claim 7). The noted language merely discloses the following:

> Once four values are read into an encryption pipeline, corresponding second data blocks must be read in a predetermined order to ensure proper feedback-type encryption. Because more data blocks are present in the sequences corresponding to contexts 400-1 to 400-4, data blocks A2, B2, C2 and D2 are input at times t5 to t8. At the same time, encrypted data values E_{KA} [A1,IVA], E_{KB} [B1,IVB], E_{KC} [C1,IVC] and E_{KD} [D1,IVD] are provided as output values and, internal to the encryption circuit, as feedback values for combination with data blocks A2, B2, C2 and D2, respectively.
>
> A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority.

The Examiner is also not correct that col. 5, lines 7-12 discloses that the one hardware cycle is approximately ten clock cycles (claim 9). The noted language merely discloses the following:

> The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

The Examiner is also not correct that col. 5, lines 7-12 discloses that the hardware implementation of the crypto-function computes an iterated round function in one clock cycle (claim 11). Again, the noted language merely discloses the following:

> The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

Accordingly, Applicants respectfully request that the above-noted rejection under 35 U.S.C. § 102(e) should be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that all of the claims are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue. The Examiner is invited to contact the undersigned at the telephone number listed below, if needed.

Respectfully submitted,
J. L. CALVIGNAC et al.

Andrew M. Calderon
Reg. No. 38,093

July 24, 2006
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
703-716-1191